# Exam Questions 2V0-41.23

VMware NSX 4.x Professional

https://www.2passeasy.com/dumps/2V0-41.23/

**NEW QUESTION 1**
What should an NSX administrator check to verify that VMware Identity Manager Integration Is successful?

A. From VMware Identity Manager the status of the remote access application must be green.
B. From the NSX UI the status of the VMware Identity Manager Integration must be "Enabled".
C. From the NSX CLI the status of the VMware Identity Manager Integration must be "Configured".
D. From the NSX UI the URI in the address bar must have "locaNfatse" part of it.

**Answer:** B

**Explanation:**
From the NSX UI the status of the VMware Identity Manager Integration must be “Enabled”. According to the VMware NSX Documentation1, after configuring VMware Identity Manager integration, you can validate the functionality by checking the status of the integration in the NSX UI. The status should be “Enabled” if the integration is successful. The other options are either incorrect or not relevant.

**NEW QUESTION 2**
Which field in a Tier-1 Gateway Firewall would be used to allow access for a collection of trustworthy web sites?

A. Source
B. Profiles -> Context Profiles
C. Destination
D. Profiles -> L7 Access Profile

**Answer:** D

**Explanation:**
The field in a Tier-1 Gateway Firewall that would be used to allow access for a collection of trustworthy web sites is Profiles -> L7 Access Profile. This field allows the user to create a Layer 7 access profile that defines list of allowed or blocked URLs based on categories, reputation, or custom entries1. The user can then apply the L7 access profile to a firewall rule to control the traffic based on the URL filtering criteria1. The other options are incorrect because they are not related to URL filtering. The Source field specifies the source IP address or group of the firewall rule1. The Destination field specifies the destination IP address or group of the firewall rule1. The Profiles -> Context Profiles field allows the user to create a context profile that defines a list of application signatures or attributes that can be used to identify and classify network
traffic1. References: Gateway Firewall

**NEW QUESTION 3**
Which CLI command on NSX Manager and NSX Edge is used to change NTP settings?

A. get timezone
B. get time-server
C. set timezone
D. set ntp-server

**Answer:** D

**Explanation:**
The CLI command on NSX Manager and NSX Edge that is used to change NTP settings is set ntp-server. Th command allows the user to configure one or more NTP servers for time synchronization12. The other options are incorrect because they are not valid CLI commands for changing NTP settings. The get timezone and timezone commands are used to display and configure the timezone of the system1. The get
time-server command is used to display the current time server configuration1. There are no CLI commands for using RADIUS or BootP for NTP settings.
References: NSX-T Command-Line Interface
Reference, vSphere ESXi 7.0 U3 and later versions NTP configuration steps

**NEW QUESTION 4**
How does the Traceflow tool identify issues in a network?

A. Compares the management plane configuration states containing control plane traffic and error reporting from transport node agents.
B. Compares intended network state in the control plane with Tunnel End Point (TEP) keepalives in the data plane.
C. Injects ICMP traffic into the data plane and observes the results in the control plane.
D. Injects synthetic traffic into the data plane and observes the results in the control plane.

**Answer:** D

**Explanation:**
The Traceflow tool identifies issues in a network by injecting synthetic traffic into the data plane and observing the results in the control plane. This allows the tool to identify any issues in the network and provide a detailed report on the problem. You can use the Traceflow tool to test connectivity between any two endpoints in your NSX-T Data Center environment.

**NEW QUESTION 5**
Which command is used to display the network configuration of the Tunnel Endpoint (TEP) IP on a bare metal transport node?

A. tepconfig
B. ifconfig
C. tcpdump
D. debug

**Answer:** B

**Explanation:**
The command ifconfig is used to display the network configuration of the Tunnel Endpoint (TEP) IP on a ba metal transport node2. The TEP IP is assigned to a network interface on the bare metal server that is used for overlay traffic. The ifconfig command can show the IP address, netmask, broadcast address, and other information of the network interface. For example, the following command shows the network configuration
of the TEP IP on a bare metal transport node with interface name ens192:
ifconfig ens192
The output of the command would look something like this:
ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 10.10.10.10 netmask 255.255.255.1 broadcast 10.10.10.255 inet6 fe80::250:56ff:fe9a:1b8c prefixlen 64 scopeid 0x20<link> ether 00:50:56:9a:1b:8c txqueuelen 1000 (Ethernet) RX packets 123456 bytes 123456789 (123.4 MB) RX errors 0
dropped 0 overruns 0 frame 0 TX packets 234567 bytes 234567890 (234.5 MB) TX errors 0 dropped 0
overruns 0 carrier 0 collisions 0
The TEP IP in this example is 10.10.10.10. References:

- IBM Cloud Docs

**NEW QUESTION 6**
When deploying an NSX Edge Transport Node, what two valid IP address assignment options should be specified for the TEP IP addresses? (Choose two.)

A. Use an IP Pool
B. Use a DHCP Server
C. Use RADIUS
D. Use a Static IP List
E. Use BootP

**Answer:** AD

**Explanation:**
When deploying an NSX Edge Transport Node, two valid IP address assignment options that should be specified for the TEP IP addresses are Use an IP Pool and Use a Static IP List. These options allow the u assign TEP IP addresses from a predefined range of IP addresses or a manually entered list of IP addresses, respectively345. The other options are incorrect because they are not supported methods for assigning TEP IP addresses. There is no option to use a DHCP server, RADIUS, or BootP for TEP IP address assignment in NSX-T345. References: NSX-T Edge TEP networking options, Multi-TEP High Availability, Create an Pool for Host Tunnel Endpoint IP Addresses

**NEW QUESTION 7**
Where in the NSX UI would an administrator set the time attribute for a time-based Gateway Firewall rule?

A. The option to set time-based rule is a clock Icon in the rule.
B. The option to set time based rule is a field in the rule Itself.
C. There Is no option in the NSX U
D. It must be done via command line interface.
E. The option to set time-based rule is a clock Icon in the policy.

**Answer:** D

**Explanation:**
According to the VMware documentation1, the clock icon appears on the firewall policy section that you want to have a time window. By clicking the clock icon, you can create or select a time window that applies to all the rules in that policy section. The other options are incorrect because they either do not exist or are not related to the time-based rule feature. There is no option to set a time-based rule in the rule itself, as it is a policy-level setting. There is also an option to set a time-based rule in the NSX UI, so it does not require using the command line interface.
https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-8572496E-A60E-48C3-A016-4A081AC8

**NEW QUESTION 8**
Which three protocols could an NSX administrator use to transfer log messages to a remote log server? (Choose three.)

A. HTTPS
B. TCP
C. SSH
D. UDP
E. TLS
F. SSL

**Answer:** BDE

**Explanation:**
An NSX administrator can use TCP, UDP, or TLS protocols to transfer log messages to a remote log server. These protocols are supported by NSX Manager, NSX Edge, and hypervisors for remote logging. A Log Insight log server supports all these protocols, as well as LI and LI-TLS, which are specific to Log Insight and optimize network usage. HTTPS, SSH, and SSL are not valid protocols for remote logging in NSX-T Data Center. References: : VMware NSX-T Data Center Administration Guide, page 102. : VMware Docs: Configure Remote Logging

**NEW QUESTION 9**
Where does an administrator configure the VLANs used In VRF Lite? (Choose two.)

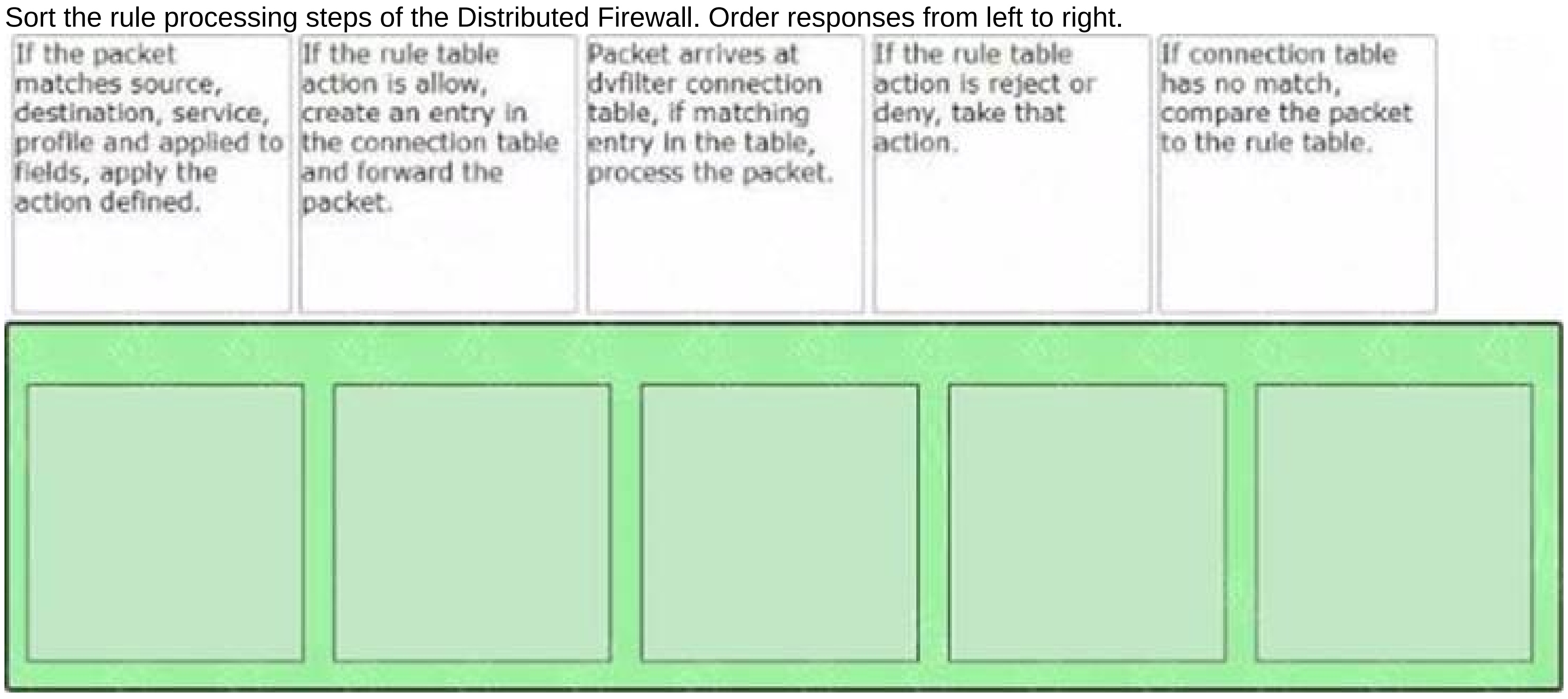
A. segment connected to the Tler-1 gateway
B. uplink trunk segment
C. downlink interface of the default Tier-0 gateway
D. uplink Interface of the VRF gateway
E. uplink interface of the default Tier-0 gateway

**Answer:** BD

**Explanation:**
According to the VMware NSX Documentation, these are the two places where you need to configure the VLANs used in VRF Lite:

- Uplink trunk segment: This is a segment that connects a tier-0 gateway to a physical network using multiple VLAN tags. You need to configure the VLAN IDs for each VRF on this segment.
- Uplink interface of the VRF gateway: This is an interface that connects a VRF gateway to an uplink trunk segment using a specific VLAN tag. You need to configure the VLAN ID for each VRF on this interface.

**NEW QUESTION 10**
Sort the rule processing steps of the Distributed Firewall. Order responses from left to right.



If the packet matches source, destination, service, profile and applied to fields, apply the action defined.

If the rule table action is allow, create an entry in the connection table and forward the packet.

Packet arrives at dvfilter connection table, if matching entry in the table, process the packet.

If the rule table action is reject or deny, take that action.

If connection table has no match, compare the packet to the rule table.

A. Mastered
B. Not Mastered

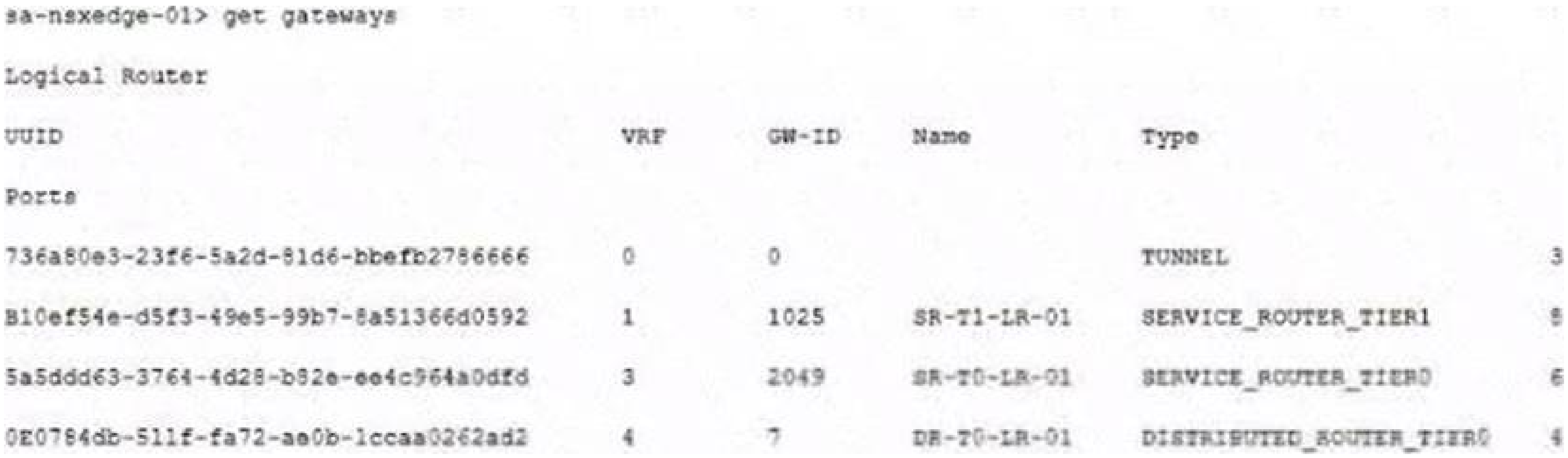
**Answer:** A

**Explanation:**
The correct order of the rule processing steps of the Distributed Firewall is as follows:

- Packet arrives at vfilter connection table. If matching entry in the table, process the packet.
- If connection table has no match, compare the packet to the rule table.
- If the rule table action is allow, create an entry in the connection table and forward the packet.
- If the rule table action is reject or deny, take that action.

This order is based on the description of how the Distributed Firewall works in the web search results1. The first step is to check if there is an existing connection entry for the packet in the vfilter connection table, which is a cache of flow entries for rules with an allow action. If there is a match, the packet is processed according to the connection entry. If there is no match, the packet is compared to the rule table, which contains all the security policy rules. The rules are evaluated from top to bottom until a match is found. The match criteria include source, destination, service, profile and applied to fields. The action defined by the matching rule is applied to the packet. The action can be allow, reject or deny. If the action is allow, a new connection entry is created for the packet and the packet is forwarded to its destination. If the action is reject or deny, the packet is dropped and an ICMP message or a TCP reset message is sent back to the source.

**NEW QUESTION 10**
A customer has a network where BGP has been enabled and the BGP neighbor is configured on the Tier-0 Gateway. An NSX administrator used the get gateways command to retrieve this Information:



```
sa-nsxedge-01> get gateways

Logical Router

UUID                                      VRF     GW-ID    Name          Type

Ports

736a80e3-23f6-5a2d-81d6-bbefb2786666      0       0                      TUNNEL                      3

B10ef54e-d5f3-49e5-99b7-8a51366d0592      1       1025     SR-T1-LR-01   SERVICE_ROUTER_TIER1        8

5a5ddd63-3764-4d28-b82e-ee4c964a0dfd      3       2049     SR-T0-LR-01   SERVICE_ROUTER_TIER0        6

0E0784db-511f-fa72-ae0b-1ccaa0262ad2      4       7        DR-T0-LR-01   DISTRIBUTED_ROUTER_TIER0    4
```

Which two commands must be executed to check BGP neighbor status? (Choose two.)

A. vrf 1
B. vrf 4
C. sa-nexedge-01(tier1_sr> get bgp neighbor
D. sa-nexedge-01(tier0_sr> get bgp neighbor
E. sa-nexedge-01(tier1_dr)> get bgp neighbor
F. vrf 3

**Answer:** DF

**Explanation:**
BGP will be configured on the T0 SR. Connect to the VRF for the T0 SR and run get bgp neighbor once connected to it.
https://docs.vmware.com/en/VMware-Validated-Design/5.1/sddc-deployment-of-vmware-nsx-t-workload-doma
For the BGP configuration on NSX-T, the Tier-0 Service Router (SR) is typically where BGP is configured. To check the BGP neighbor status:
Connect to the VRF for the T0 SR, which is VRF 3 based on the provided output. Run the command to get BGP neighbor status once connected to it.

**NEW QUESTION 13**
When a stateful service is enabled for the first lime on a Tier-0 Gateway, what happens on the NSX Edge node'

A. SR is instantiated and automatically connected with DR.
B. DR Is instantiated and automatically connected with SR.
C. SR and DR Is instantiated but requites manual connection.
D. SR and DR doesn't need to be connected to provide any stateful services.

**Answer:** A

**Explanation:**
The answer is A. SR is instantiated and automatically connected with DR.
SR stands for Service Router and DR stands for Distributed Router. They are components of the NSX Edge node that provide different functions1
The SR is responsible for providing stateful services such as NAT, firewall, load balancing, VPN, and DHCP. The DR is responsible for providing distributed routing and switching between logical segments and the physical network1
When a stateful service is enabled for the first time on a Tier-0 Gateway, the NSX Edge node automatically creates an SR instance and connects it with the existing DR instance. This allows the stateful service to be applied to the traffic that passes through the SR before reaching the DR2
According to the VMware NSX 4.x Professional Exam Guide, understanding the SR and DR components and their functions is one of the exam objectives3
To learn more about the SR and DR components and how they work on the NSX Edge node, you can refer to the following resources:

- VMware NSX Documentation: NSX Edge Components 1
- VMware NSX 4.x Professional: NSX Edge Architecture
- VMware NSX 4.x Professional: NSX Edge Routing

**NEW QUESTION 15**
What is the VMware recommended way to deploy a virtual NSX Edge Node?

A. Through the OVF command line tool
B. Through the vSphere Web Client
C. Through automated or Interactive mode using an ISO
D. Through the NSXUI

**Answer:** D

**Explanation:**
Through the NSX UI. According to the VMware NSX Documentation2, you can deploy NSX Edge nodes as virtual appliances through the NSX UI by clicking Add Edge Node and providing the required information. The other options are either outdated or not applicable for virtual NSX Edge nodes.
https://docs.vmware.com/en/VMware-NSX/4.1/installation/GUID-E9A01C68-93E7-4140-B306-19CD6806199

**NEW QUESTION 16**
Which two BGP configuration parameters can be configured in the VRF Lite gateways? (Choose two.)

A. Graceful Restart
B. BGP Neighbors
C. Local AS
D. Route Distribution
E. Route Aggregation

**Answer:** BD

**Explanation:**
According to the VMware NSX Documentation1, you can configure BGP neighbors for VRF-Lite by specifying the neighbor IP address, remote AS number, source IP address, and route filter. You can also configure route distribution for VRF-Lite by selecting the route redistribution sources and the route map to apply.
https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-4CB5796A-1CED-4F0E-A

**NEW QUESTION 18**
What needs to be configured on a Tler-0 Gateway lo make NSX Edge Services available to a VM on a VLAN-backed logical switch?

A. Downlink Interface
B. VLAN Uplink
C. Loopback Router Port
D. Service Interface

**Answer:** B

**Explanation:**
To make NSX Edge Services available to a VM on a VLAN-backed logical switch, you need to configure
a VLAN Uplink on the Tier-0 Gateway. A VLAN Uplink is a logical interface that connects the Tier-0 Gateway to the physical network and provides external connectivity for the NSX Edge Services1. A VLAN Uplink can be configured on the NSX Manager UI by selecting Networking > Tier-0 Gateways > Interfaces > Set > Add Interface1.
https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-D641380B-4C8E-4C8A-AF64-4261A266

**NEW QUESTION 19**
An NSX administrator has deployed a single NSX Manager node and will be adding two additional nodes to form a 3-node NSX Management Cluster for a production environment. The administrator will deploy these two additional nodes and Cluster VIP using the NSX UI.
What two are the prerequisites for this configuration? (Choose two.)

A. All nodes must be in separate subnets.
B. The cluster configuration must be completed using API.
C. NSX Manager must reside on a Windows Server.
D. All nodes must be in the same subnet.
E. A compute manager must be configured.

**Answer:** DE

**Explanation:**
According to the VMware NSX Documentation, these are the prerequisites for adding nodes to an NSX Management Cluster using the NSX UI:

- All nodes must be in the same subnet and have IP connectivity with each other.
- A compute manager must be configured and associated with the NSX Manager node.
- The NSX Manager node must have a valid license.
- The NSX Manager node must have a valid certificate.

**NEW QUESTION 24**
As part of an organization's IT security compliance requirement, NSX Manager must be configured for 2FA (two-factor authentication).
What should an NSX administrator have ready before the integration can be configured? O

A. Active Directory LDAP integration with OAuth Client added
B. VMware Identity Manager with an OAuth Client added
C. Active Directory LDAP integration with ADFS
D. VMware Identity Manager with NSX added as a Web Application

**Answer:** B

**Explanation:**
To configure NSX Manager for two-factor authentication (2FA), an NSX administrator must have VMware
Identity Manager (vIDM) with an OAuth Client added. vIDM provides identity management services and supports various 2FA methods, such as VMware Verify, RSA SecurID, and RADIUS. An OAuth Client is a configuration entity in vIDM that represents an application that can use vIDM for authentication and authorization. NSX Manager must be registered as an OAuth Client in vIDM before it can use
2FA. References: : VMware NSX-T Data Center Installation Guide, page 19. : VMware NSX-T Data Center Administration Guide, page 102. : VMware Blogs: Two-Factor Authentication with VMware NSX-T

**NEW QUESTION 29**
Which three selections are capabilities of Network Topology? (Choose three.)

A. Display how the different NSX components are interconnected.
B. Display the uplink configured on the Tier-0 Gateways.
C. Display how the Physical components ate interconnected.
D. Display the VMs connected to Segments.
E. Display the uplinks configured on the Tier-1 Gateways.

**Answer:** ABD

**Explanation:**
According to the VMware NSX Documentation, these are three of the capabilities of Network Topology, which is a graphical representation of your network infrastructure in NSX:

- Display how the different NSX components are interconnected: You can use Network Topology to view how your segments, gateways, routers, firewalls, load balancers, VPNs, and other NSX components are connected and configured in your network.
- Display the uplink configured on the Tier-0 Gateways: You can use Network Topology to view the uplink interface and segment that connect your tier-0 gateways to your physical network. You can also view the VLAN ID and IP address of the uplink interface.
- Display the VMs connected to Segments: You can use Network Topology to view the VMs that are attached to your segments. You can also view the IP address and MAC address of each VM.

**NEW QUESTION 31**
Which two statements are correct about East-West Malware Prevention? (Choose two.)

A. A SVM is deployed on every ESXi host.
B. NSX Application Platform must have Internet access.
C. An agent must be installed on every ESXi host.
D. An agent must be installed on every NSX Edge node.
E. NSX Edge nodes must have Internet access.

**Answer:** AE

**Explanation:**
East-West Malware Prevention is a feature of NSX Advanced Threat Prevention that can detect and prevent malicious files in the network traffic between virtual machines (east-west) and between the data center and the external network (north-south). To enable this feature, a Service Virtual Machine (SVM) is deployed on every ESXi host to intercept and analyze the files in the east-west traffic. An agent must also be installed on every NSX Edge node to intercept and analyze the files in the north-south traffic. The NSX Application Platform is a cloud-based service that provides threat intelligence and analysis for the NSX Malware Prevention feature. The NSX Application Platform must have Internet access to receive updates and send files for analysis. The NSX Edge nodes must also have Internet

access to communicate with the NSX Application Platform.
References:

- Overview of NSX IDS/IPS and NSX Malware Prevention
- Administering NSX Malware Prevention

**NEW QUESTION 36**
Which NSX CLI command is used to change the authentication policy for local users?

A. Set cli-timeout
B. Get auth-policy minimum-password-length
C. Set hardening- policy
D. Set auth-policy

**Answer:** D

**Explanation:**
According to the VMware NSX Documentation4, the set auth-policy command is used to change the authentication policy settings for local users, such as password length, lockout period, and maximum authentication failures. The other commands are either used to view the authentication policy settings (B), change the CLI session timeout (A), or change the hardening policy settings ©.

**NEW QUESTION 38**
When collecting support bundles through NSX Manager, which files should be excluded for potentially containing sensitive information?

A. Controller Files
B. Management Files
C. Core Files
D. Audit Files

**Answer:** C

**Explanation:**
According to the VMware NSX Documentation1, core files and audit logs can contain sensitive information and should be excluded from the support bundle unless requested by VMware technical support. Controller files and management files are not mentioned as containing sensitive information.

**NEW QUESTION 42**
Which steps are required to activate Malware Prevention on the NSX Application Platform?

A. Select Cloud Region and Deploy Network Detection and Response.
B. Activate NSX Network Detection and Response and run Pre-checks.
C. Activate NSX Network Detection and Response and Deploy Malware Prevention.
D. Select Cloud Region and run Pre-checks.

**Answer:** D

**Explanation:**
To activate Malware Prevention on the NSX Application Platform, the steps are:

- In the NSX Manager UI, select System and in the Configuration section, select NSX Application Platform.
- Navigate to the Features section, locate the NSX Malware Prevention feature card, and click Activate or anywhere in the card.
- In the NSX Malware Prevention activation window, select one of the available cloud regions from which you can access the NSX Advanced Threat Prevention cloud service.
- Click Run Prechecks. This precheck process can take some time as the system validates that the minimum license requirement is met and that it is eligible for use with the NSX Advanced Threat Prevention cloud service. The system also validates that the selected cloud region is reachable.
- Click Activate. This step can take some time1. Therefore, the correct answer is D. The other options are incorrect because they involve activating or deploying NSX Network Detection and Response, which is
a different feature from Malware Prevention. References: Activate NSX Malware Prevention

**NEW QUESTION 43**
Which two statements describe the characteristics of an Edge Cluster in NSX? (Choose two.)

A. Can have a maximum of 8 edge nodes
B. Can have a maximum of 10 edge nodes
C. Must have only active-active edge nodes
D. Can contain multiple types of edge nodes (VM or bare metal)
E. Must contain only one type of edge nodes (VM or bare metal)

**Answer:** AE

**Explanation:**
Two statements that describe the characteristics of an Edge Cluster in NSX are:

- An Edge Cluster can have a maximum of 8 edge nodes2. This is the upper limit for scaling out the Edge Cluster and providing high availability and load balancing for network services.
- An Edge Cluster must contain only one type of edge nodes (VM or bare metal)3. This is because different types of edge nodes have different performance and resource requirements, and mixing them in the same cluster can cause inconsistency and instability. The other options are incorrect because they do not describe the characteristics of an Edge Cluster in NSX. An Edge Cluster can have either
active-active or active-standby edge nodes, depending on the configuration and services4. An Edge Cluster cannot contain multiple types of edge nodes, as explained above. References: Enhanced NSX Edge and Networking Services in NSX 4.0.1.1, NSX Edge Installation Requirements, NSX-T Edge Node Cluster

**NEW QUESTION 46**
What are two valid BGP Attributes that can be used to influence the route path traffic will take? (Choose two.)

A. AS-Path Prepend
B. BFD
C. Cost
D. MED

**Answer:** AD

**Explanation:**

> AS-Path Prepend: This attribute allows you to prepend one or more AS numbers to the AS path of a route, making it appear longer and less preferable to other BGP routers. You can use this attribute to manipulate the inbound traffic from your BGP peers by advertising a longer AS path for some routes and a shorter AS path for others .

> MED: This attribute stands for Multi-Exit Discriminator and allows you to specify a preference value for a route among multiple exit points from an AS. You can use this attribute to manipulate the outbound traffic to your BGP peers by advertising a lower MED value for some routes and a higher MED value for others .

**NEW QUESTION 50**
......